The GDPR and algorithmic decision-making

Safeguarding individual rights, but forgetting society

Völkerrechtsblog 2019-06-03T11:00:07

In algorithmic decision-making systems (ADM systems) machines evaluate and assess human beings and, on this basis, make a decision or provide a forecast or a recommendation for action. Thus, it is not only the data processing as such, but above all the automated decision resulting from the data processing that contains risks for the user. The current international legal framework encompasses such risks by guaranteeing privacy, data protection, personality rights and autonomy. However, there are group-related and societal interests such as fairness, non-discrimination, social participation and pluralism. In order to attain such supraindividual goals, experts have suggested the adoption of certain measures which contribute to making ADM procedures transparent, individual decisions explainable and revisable, as well as to making the systems verifiable and rectifiable. Furthermore, ensuring the diversity of ADM systems can make a contribution to safeguarding the mentioned interests.

Against this background and in light of the growing use of ADM systems we need to ask ourselves an important question: To what extent can the EU General Data Protection Regulation (GDPR) support such measures and protect the interests of the individual, of groups and of society as whole that seem threatened by algorithmic systems?

GDPR's prohibition of ADM systems: Limited scope and broad exceptions

As a matter of fact, Art. 22 (1) GDPR does prohibit automated decision making by stating that any "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling". However, in a legal analysis – see this 2019 full report – we demonstrate that the GDPR's room for manoeuvre in the area of ADM systems is quite restricted. This is a short summary of the findings, showing that in the small area of permitted ADM cases Art. 22 GDPR can create transparency and verifiability and thus help to safeguard individual rights. However, regarding group-related and societal goals such as non-discrimination and participation the GDPR has little to offer. For this reason, there is a need to discuss complementary regulatory tools beyond the GDPR.

The application of the GDPR's prohibition of ADM systems is, for a variety of reasons, closely restricted. The GDPR prohibits only fully automated decision-making. Systems which "only" prepare the basis for human decisions and give recommendations may still very well be used. For the prohibition to come into effect,

ADM systems must make fully automated decisions on the basis of personal data, plus the decisions must have legal consequences or similarly affect the data subject significantly. If one of these three criteria is missing, the ADM-specific provisions in Art. 22 GDPR do not apply. Here, it is unclear in the case of ADM systems what a “decision” actually is, and under what circumstances it produces “legal effects”. Moreover, the regulation can hardly encompass the diversity of actual decision-making situations in which people consciously or unconsciously implement an automated decision or recommendation more or less unquestioningly. Both the relatively narrow scope of application of the prohibition and the broad range of legal exceptions to the prohibition provided in Art. 22 (2) GDPR – first and foremost on basis of consent given by the data subject – result in very limited cases in which an ADM system is *actually* prohibited. Hence, (partly) automated decisions are going to become a normal part of our everyday digital lives.

Information duties regarding the “logic involved” in permitted ADM systems

For ADM systems that are “exceptionally” permissible under the GDPR the regulation contains legal provisions which can partly safeguard the individual interests of the users: Data controllers of ADM systems are subject to ex ante transparency rules relating to the use of ADM systems (Art. 13, 14 GDPR) as well as to ex-post information obligations regarding the basic mechanisms of data processing and decision-making in case of a user exerting her right to information. The duty to provide information about the “how” of an ADM System (i.e., the “logic involved” and the “significance and consequences of data processing” within the framework of automated decision-making) is what allows for the individual’s possibility of exerting informational self-determination. While it is generally agreed that the wording of Art. 13 (2) f) and Art. 14 (2) g) GDPR specify a duty to inform the data subject of the intent to use data processing in making an automated decision, it remains unclear how far the duty to provide transparency in automated decision-making with regard to the “logic involved” and the “significance and consequences of data processing” goes. It specifically remains unclear what the notion of “logic involved” in Art. 13 (2) f) and Art. 14 (2) g) actually means. Some (international) legal researchers believe that this constitutes a duty to disclose the source code, whereas others interpret the stipulation as a fundamental duty to use explainable ADM systems. Others argue that in view of the data controllers’ interests in secrecy, there is merely a duty to provide (only) abstract information about the workings and criteria applied by an automated decision-making system.

Despite the outcome of these debates, the regulation is determined to solely focus on the data protection of the individual. For this reason, the scope and comprehensibility of the explanation of both the “logic involved” as well as the “significance and the envisaged consequences” of the ADM decision is based on and limited by the perspective and cognitive skills of the average user. Moreover, transparency provisions aiming at data subjects do not automatically lead to higher levels of basic rights protection in practical terms. Regarding ADM systems data subjects have a right to disclosure about the use of an ADM system in general as well as regarding the basic mechanisms of data processing and decision-making. Furthermore, they have the right to obtain human intervention (Art. 22 (3) GDPR).

These rights, too, help to safeguard individual rights and freedoms. They make it possible to verify and – if needed – to overrule the automated decision. However, this does not constitute a right for data subjects or for independent third parties to scrutinize the whole ADM system including its inner workings.

Positive potentials of systemic GDPR provisions

Systemic and procedural GDPR provisions regarding the design and implementation of ADM systems can help the data controller to detect risks for the individual (and indirectly for groups) at an early stage and to ensure minimum quality standards. Such rules include privacy by design obligations (Art. 25 (1) GDPR), obligatory data protection impact assessments (Art. 35 (3) a) GDPR) and binding corporate rules (Art. 47 (2) lit. e GDPR), as well as the appointment of a data protection officer (Art. 37 GDPR). These regulatory tools have the potential to create a high level of awareness with the data controller regarding data protection issues, and thus helping to safeguard individual rights and freedoms. Such controller-related duties can in theory be strengthened in addition by the data protection authorities, who are granted encompassing disclosure and access rights. They can scrutinize ADM processes and carry out impact assessments during data protection audits. However, the focus of these audits is, again, only the protection of individual rights.

GDPR's focus on individual rights neglects group-related and societal interests in ADM

Taken as a whole, the GDPR does not offer great potential when it comes to protecting group-related and societal interests such as non-discrimination, participation or pluralism. A prerequisite for this would be the option for an external inspection of the internal design of the ADM systems in order to be able to evaluate independently its basic concepts and processes. However, the GDPR transparency rules cannot facilitate such a deep insight into the system. Thus, it is not possible to uncover errors or misconceptions in the development and implementation of ADM systems as well as their potential effects on social interactions.

Moreover, an overview over the actual diversity of ADM systems is difficult to acquire against the background of system-related intransparency. In order to protect group-related and societal interests as well as to improve system-related transparency and external evaluation, there is a need for complementary approaches. For this purpose, certain measures within the GDPR might be strengthened. For example, the data protection authorities could also require data protection impact assessments according to Art. 35 (4) GDPR for all cases of ADM systems, specifically including those that are not covered by Art. 22 GDPR. This would make it possible to identify risks at an early stage and to guarantee minimum protection standards. Furthermore, within the framework of the GDPR the role of the data protection authorities could shift towards more public information and awareness building regarding potential societal problems, even if the authorities do not have enforcement powers that go beyond dealing with data protection infringements.

Protecting supraindividual rights and interests: Thinking beyond the Regulation

Other regulatory tools beyond the scope of the GDPR will have to be discussed in order to be able to safeguard both supraindividual and societal goals. In order to improve the inspection of ADM systems, certain approaches can contribute to the greater explainability of the systems. In case such systems are already in use, enhanced transparency requirements could provide for better external assessment, e.g. in the form of in-camera proceedings that protect the interests and confidentiality of the data controller. In order to rectify ADM systems already implemented, it seems possible to use regulatory tools from competition law and consumer protection law, since they might result in faster forms of enforcement. The diversity of ADM systems can be supported by adopting regulatory tools provided by cartel law. Furthermore, media law requirements could contribute to pluralism in the case of ADM systems that have an effect on information access and that influence public opinion formation.

Since the GDPR primarily focuses on safeguarding individual rights and freedoms, the regulation's potential for shaping international regulatory standards is limited when it comes to implementing supraindividual rights and interests.

Dr. Stephan Dreyer is Senior Researcher for Media Law and Media Governance at the Leibniz-Institute for Media Research | Hans-Bredow-Institut (HBI), Hamburg.

Prof. Dr. Wolfgang Schulz is Director of the HBI.

This contribution is based on a study by the authors: Stephan Dreyer and Wolfgang Schulz (2019), The General Data Protection Regulation and Automated Decision-making: Will it deliver?, Potentials and limitations in ensuring the rights and freedoms of individuals, groups and society as a whole, Discussion Paper Ethics of Algorithms #5, https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/GDPR.pdf

Cite as: Stephan Dreyer & Wolfgang Schulz, "The GDPR and algorithmic decision-making – Safeguarding individual rights, but forgetting society", *Völkerrechtsblog*, 3 June 2019.